臺東縣立大武國中
資通安全管理系統
實施原則

幹事洪國欽　教務主任簡世隆　臺東縣立大武國民中學校長許志民

中 華 民 國 105 年 03 月 01 日

適用範圍

1. 學校內電腦、資訊與網路服務相關的系統、設備、程序、及人員。
2. 學生用電腦：電腦教室及各專科教室內提供學生操作使用的電腦設備。
3. 教師用電腦：教職員工個人專用的教學或行政用電腦設備。
4. 教師公用電腦：辦公室中供所有教師共同使用的電腦設備。

一、 實施原則

1. 網路安全

1.1 網路控制措施

- 學校與外界連線，完全經由縣網中心之管控，以符合一致性與單一性之安全要求。
- 本校不提供以電話線連結主機電腦或網路設備。

1.2 網路安全管理服務委外廠商合約之安全要求

- 委外開發或維護廠商必須簽訂安全保密切結書（文件編號 A-1）。

2. 系統安全

2.1 職責區隔

- 學校主機電腦依個別應用系統之需要，設置專屬電腦，例如：網路服務主機（網站主機、檔案伺服器）。
- 學校的行政系統主機（例如財務、人事、公文、會計、學務行政系統等）電腦，都由臺東縣教育網路中心或臺東縣政府相關單位統籌管理。

2.2 對抗惡意軟體、隱密通道及特洛依木馬程式

- 學生用電腦：
  - 使用還原卡，每次開機都會自動還原系統。
  - 裝置防毒軟體，將軟體設定為自動定期更新病毒碼。
  - 每年一次進行所有程式之更新作業，以防範所有系統之漏洞。
- 教師用電腦、教師公用電腦及伺服器
  - 裝置防毒軟體，將軟體設定為自動定期更新病毒碼。
  - 系統設定自動進行如「Windows Update」之程式更新作業，以防範作業系統之漏洞。
- 學校內個人電腦所使用的軟體應有合法授權，並於校務會議中宣導。

- 新系統啟用前，須經過掃毒與更新系統密碼程序，以防範可能隱藏的病毒或後門程式。

2.3 資料備份

- 學校(或委託)系統管理人員需針對學校重要系統（例如系統檔案、應用系統、資料庫等）定期進行備份工作，或採用自動備份機制；週期為每月進行一次或資料有更改時同時進行備份。
- 學校的行政系統主機（例如財務、人事、公文、人事、校務行政系統等）電腦，都由臺東縣教育網路中心或臺東縣政府相關單位統籌資料備份工作。

2.4 操作員日誌

- 學校(或委託)系統管理人員需針對敏感度高、或包含特殊資訊的電腦系統進行檢查、維護、更新等動作時，須針對這些活動填寫日誌予以紀錄，作為未來需要時之檢查。
- 日誌內容可包含以下各項：
  - 系統例行檢查、維護、更新活動的起始時間
  - 系統錯誤內容和採取的改正措施。[*文件編號 A-2*]
  - 紀錄日誌項目人員姓名與簽名欄

2.5 資訊存取限制

- 學校內所共用的個人電腦應以特定功能為目的，並設定特定安全管控機制（例如限制從網路非法下載檔案行為、限制自行安裝軟體行為、限制特定資料的存取等）。

2.6 使用者註冊

- 學校制定電腦系統使用的使用者註冊及註銷程序，透過該註冊及註銷程序來控制使用者資訊服務的存取，該作業應包括以下內容：
  - 使用唯一的使用者識別碼（ID）。
  - 檢查使用者是否經過系統管理單位之授權使用資訊系統或服務。
  - 保存一份包含所有識別碼註冊的記錄。
  - 使用者調職或離職後，由資訊組長移除其識別碼的存取權限。
  - 每學年檢查並取消多餘的使用者識別碼和帳號。
  - 每學年檢查新增之帳號，若有莫名帳號產生，關閉帳號權限，並依通報程序請求處理（參照本文件 2.10 段落）。

2.7 特權管理

- 學校的電腦與網路系統資訊具有存取特權人員清單、及其所持有的權限說明，每學期建立清冊記錄備查。

2.8 通行碼之使用

- 教師用電腦、教師公用電腦及伺服器均設有專屬帳號及通行碼。
- 管制使用者第一次登入系統時，必須立即更改預設通行碼，預設通行碼應設定有效期限。
- 由學校發佈通行碼（Password）制定與使用規則給使用者，[*文件編號 A-3*]，內容包含以下各項：
  - 使用者對其個人所持有通行碼盡保密責任
  - 要求使用者的通行碼設定，避免使用易於猜測之數字或文字，例如生日、名字、鍵盤上聯繫的字母與數字(如 12345678 或 asdfghjk)，以及過多的重複字元等。或建議通行碼應該包含英文字大小寫、數字、特殊符號等四種設定中的三種。
- 因特殊需要擁有多個帳號時，可考慮使用一組複雜但相同的通行碼。

2.9 原始程式庫之存取控制

- 學校與系統廠商間的合約須加註對原始程式庫安全之要求，並防範資料庫隱碼(SQL-injection)問題，針對存取資料庫程式碼之輸入欄位進行字元合理性檢查。

2.10 通報安全事件與處理

- 資訊安全事件包括：任何來自網路的駭客攻擊、病毒感染、垃圾郵件、資料或網頁遭竄改、以及通訊中斷等。
- 學校須建立資訊安全事件通報程序[文件編號 *A-4*]以及安全事件通報單[*文件編號 A-5*]；通報程序包括學校內部通報，以及學校與所屬縣市教育網路中心的通報。
- 當學校內部無法處理之資通安全事件，應通報縣臺東縣網路中心。
- 所訂出資訊安全事件通報程序應公布於校園內使用電腦與網路之場所，提供使用者瞭解。

3. 實體安全

3.1 設備安置及保護

- 學校資訊設備主機機房、電腦教室區域，須設置滅火設備，並禁止擺放易燃物、或飲食。
- 學校資訊設備主機機房、電腦教室區域內的電源線插頭須有接地的連結、或有避雷針等裝置，避免如雷擊事件所造成損害情況。
- 學校資訊設備主機機房、電腦教室區域，至少於入出口處加裝門鎖或其他同等裝置。

3.2 電源供應

- 學校重要的資訊設備（如主機機房）應有適當的電力設施，例如設置UPS、電源保護措施，以免斷電或過負載而造成損失。

3.3 纜線安全

- 學校資訊設備主機機房、電腦教室區域內須避免明佈線。

3.4 設備與儲存媒體之安全報廢或再使用

- 所有包括儲存媒體的設備項目，在報廢前，應先確保已將任何敏感資料和授權軟體刪除或覆寫，並於報廢單上註記。

3.5 設備維護

- 須與設備廠商建立維護合約。
- 廠商進入安全區域(機房)需簽訂安全保密切結書[文件編號 *A-1*]。

3.6 財產攜出、入

- 未經授權不應將學校的資訊設備、資訊或軟體攜出所在地。
- 當有必要將設備移出，應檢視相關授權，並實施登記與歸還記錄。
- 相關財產之攜出應依教育部或學校既有之相關規定處理。

3.7 桌面淨空與螢幕淨空政策

- 結束工作時，所有學校教職員工應將其所經辦或使用具有機密或敏感特性的資料（例如公文、學籍資料等）及資料的儲存媒體（如 USB 隨身碟、磁碟片、光碟等），妥善存放。
- 學校提供教職員工或學生使用的個人電腦應設定保護裝置，如個人鑰匙、個人密碼以及螢幕保護。

4. 人員安全

4.1 將安全列入工作執掌中

- 應將資訊安全納入教職員手冊說明中，以強化工作上之資訊安全意識。

4.2 資訊安全教育與訓練

- 使學校(或委託)系統管理人員有足夠能力執行日常基礎之資安管理系統維護工作，並使其瞭解資安事件通報之程序。
- 學校鼓勵或安排資訊組長/老師/系統管理人員、以及所有教職員參與資訊安全教育訓練或宣導活動，以提昇資訊安全認知。

5. 應對以下各項相關法令有基礎之認知

5.1 智慧財產權

- 經濟部智慧財產局 http://www.tipo.gov.tw/
- 著作權法
  http://www.tipo.gov.tw/copyright/copyright_law/copyright_law_92.asp

5.2 個人資訊的資料保護及隱私

個人資料保護法

http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021

5.3 電子簽章法

- 電子簽章法
  http://www.moea.gov.tw/~meco/doc/ndoc/s5_p05.htm
- 電子簽章法施行細則
  http://www.moea.gov.tw/~meco/doc/ndoc/s5_p05_p01.htm
- 核可憑證機構名單
  http://www.moea.gov.tw/~meco/doc/ndoc/s5_p07_p03.htm

文件編號：A-1

臺東縣立大武國民中學資訊服務委外單位服務暨保密切結書

_____公司(以下簡稱為本公司)為配合臺東縣立大武國民中學（以下簡稱為貴校）之資訊應用業務需求，進行相關資訊系統或軟體開發、測試、建置及維護等工作。本公司提供資訊服務項目如下：

一、

二、

三、

本公司願意在對貴校提供上述服務項目範圍內之服務時，保證因提供業務服務需存取貴校資訊系統中所存放，凡屬與公文機密、個人及事業單位權益相關之資料，無論其內容之一部或全部，均負保密之責；相關資料均以留在貴校內部範疇內處理，倘須由本公司攜至校外處理，應簽奉貴校核可。

本公司亦不私自蒐集貴校所擁有之任何資訊。若所提供之資訊業務服務，不符合上述之規定或經營之服務項目超出上述範圍，或違犯法令，本公司同意無異議接受接受法律制裁與及其訴訟費用，並負責所引發之各項損失賠償。此致

臺東縣立大武國民中學

申請單位及負責人蓋章：

日期：　　年　　月　　日

本服務暨保密切結書一式兩份，分別由_____公司以及臺東縣立大武國民中學保存

文件編號：A-2

臺東縣立大武國民中學操作員日誌

填寫日期：　　民國___年___月___日

系統操作起始時間：　上（下）午___時___分

系統操作結束時間：　上（下）午___時___分

操作事項	☐ 系統例行檢查 ☐ 系統維護 ☐ 系統更新操作
系統錯誤說明	
採取改正措施說明	

操作人員：_____　　簽名欄：_____

日誌填寫人員：_____　　簽名欄：_____

教務主任：_____　　簽名欄：_____

文件編號：A-3

優質通行碼設定原則與使用原則

一、 良好的通行碼設定原則

1. 混合大寫與小寫字母、數字，特殊符號。
2. 通行碼越長越好，最短也應該在 8 個字以上。
3. 至少每三個月改一次密碼。
4. 使用技巧記住通行碼
   - 使用字首字尾記憶法：
     a. My favorite student is named Sophie Chen，取字頭成為 mFSinsC
     b. There are 26 lovely kids in my English class，取字尾成為 Ee6ysnMEc
   - 中文輸入按鍵記憶法：
     a. 例如「通行碼」的注音輸入為「wj/ vu/6a83」

二、 應該避免的作法

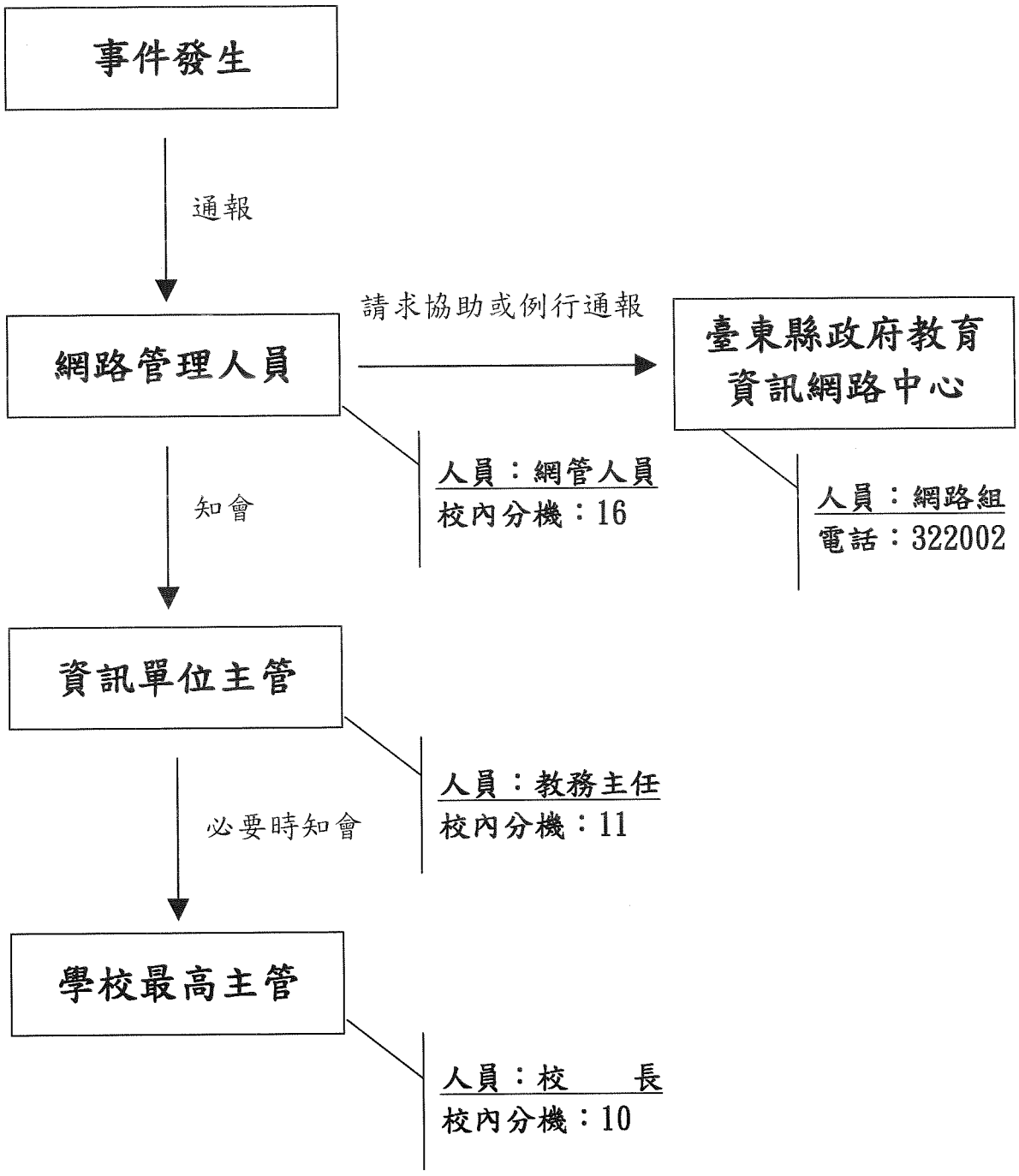
1. 嚴禁不設通行碼
2. 通行碼嚴禁與帳號相同
3. 通行碼嚴禁與主機名稱相同
4. 不要使用與自己有關的資訊，例如學校或家裡電話、親朋好友姓名、身份證號碼、生日等。
5. 不重覆電腦鍵盤上的字母，例如 6666rrrr 或 qwertyui 或 zxcvbnm。
6. 不使用連續或簡單的組合的字母或數字，例如 abcdefgh 或 12345678 或 24681024
7. 避免全部使用數字，例如 52526565
8. 不使用難記以至必須寫下來的通行碼。
9. 避免使用字典找得到的英文單字或詞語，如 TomCruz 、superman
10. 不要使用電腦的登入畫面上任何出現的字。
11. 不分享通行碼內容給任何人，包括男女朋友、職務代理人、上司等。

延伸參考：

"Password Management Guideline", by department of defense computer security center, 12 April 1985 http://www.radium.ncsc.mil/tpep/library/rainbow/CSC-STD-002-85.pdf

文件編號：A-4

安全事件通報程序



文件編號：A-5

臺東縣立大武國民中學資通安全事件通報單

編號：_____

填報時間：_____年_____月_____日_____時 _____分

洽詢電話：_____ 傳真：_____

E-mail：_____

或逕送：_____

一、發生資通安全之機關(機構)聯絡資料：

機關(機構)名稱：_____聯絡人：_____

E-mail：_____

電話：_____ 傳真：_____

二、資通安全事件通報事項：

1.事件發生時間：_____年____月____日_____時_____分

2.主機(伺服器)資料：

◎ IP 位址(IP Address)：_____

◎ 網域名稱(Domain name)：_____

◎ 主機(伺服器)廠牌、機型：_____

◎ 作業系統名稱、版本、序號：_____

◎ 網際網路資訊位址(Web URL)：_____

◎ 已裝置之安全機制：_____

3.資通安全事件資料：

◎影響等級：□『A』級：影響公共安全、社會秩序、人民生命財產。

□『B』級：系統停頓，業務無法運作。

□『C』級：業務中斷，影響系統效率。

□『D』級：業務短暫停頓，可立即修復。

◎ 事件說明：

◎ 應變措施：

三、期望支援項目：

四、解決辦法：

五、已解決時間：_____年_____月_____日_____時_____分

網管人員： **教務主任：** **校長：**

臺東縣立大武國民中學資通安全事件解除單

編號：_____

填報時間：_____年_____月_____日_____時 _____分

洽詢電話：_____ 傳真：_____

E-mail：_____

或逕送：_____

一、發生資通安全之機關(機構)聯絡資料：

機關(機構)名稱：_____聯絡人：_____

E-mail：_____

電話：_____ 傳真：_____

二、資通安全事件通報事項：

1.事件發生時間：_____年____月____日_____時_____分

2.主機(伺服器)資料：

◎ IP 位址(IP Address)：_____

◎ 網域名稱(Domain name)：_____

◎ 主機(伺服器)廠牌、機型：_____

◎ 作業系統名稱、版本、序號：_____

◎ 網際網路資訊位址(Web URL)：_____

◎ 已裝置之安全機制：_____

3.資通安全事件資料：

◎影響等級： □『A』級：影響公共安全、社會秩序、人民生命財產。

□『B』級：系統停頓，業務無法運作。

□『C』級：業務中斷，影響系統效率。

□『D』級：業務短暫停頓，可立即修復。

◎ 事件說明：

◎ 應變措施：

三、已解決時間：_____年_____月_____日_____時_____分

填寫人：_____